Por Déborah Oliveira

Especialistas em segurança alertam que é preciso investir na educação dos usuários. Falta de regulamentação para vazamento de dados também reduz amplo acesso ao tema, o que poderia evitar novos episódios

Realizado hoje (10/2), o **Dia da Internet Segura** alerta e conscientiza internautas sobre a forma que usam a web. No Brasil, a ação é promovida pela SaferNet, associação civil de direito privado. Ao todo, mobilizações para reforçar o tema acontecerão em mais de cem países. Para o mundo corporativo, a data lembra cuidados que devem ser tomados na internet para evitar invasões e exposição de informações sensíveis.

Isso porque, embora exista uma ampla consciência sobre o assunto, muitas organizações ignoram recursos de proteção e posicionam a segurança como coadjuvante em suas estratégias. Pesquisa recente da Daryus, consultoria focada no treinamento de profissionais do setor, mostra que em quase 53% das companhias Sistema de Gestão de Segurança da Informação são informais ou não existem. O dado indica claramente que é preciso direcionar mais cuidados à proteção dos dados.

A McAffe, que criou para a data uma página com dicas para proteção no ambiente digital, observa que o uso de ferramentas de segurança é fundamental para fortalecer o ambiente corporativo. As tecnologias contribuem para alertar sobre problemas. Contudo, o comportamento do usuário tem grande influência na segurança, observa José Matias Neto, diretor de Suporte Técnico para América Latina da McAfee.

Assim, segundo ele, é crucial fortalecer a questão comportamental. “O usuário é o mais sensível na cadeia de segurança porque ele toma as decisões e leva a experiência de consumidor para dentro da corporação”, pontua. A preocupação com a educação do usuário é ainda maior, diz, na era do *bring your own device* (BYOD).

Diante desse cenário, Neto alerta que é necessário conscientizar os usuários. Hoje, 51% dos ataques bem-sucedidos começam com phishing enviado por e-mail para colaboradores, que muitas vezes desconhecem a tentativa de fraude.

O executivo indica ainda que o aumento do uso de wi-fi público também traz um enorme risco para a segurança. “Quem oferece wi-fi, oferece conectividade e não segurança”, alerta. De acordo com ele, o custo para proteger esses ambientes é enorme, pois não se conhece o usuário. “É importante criar consciência de que wi-fi não é seguro. Não se deve fazer transações bancárias, trocar e-mails sigilosos ou acessar sistemas críticos”, aconselha.

André Carraretto, especialista de segurança da informação da Symantec, concorda que a educação merece destaque na estratégia de proteção. “Por mais que a organização tenha soluções, ataques virtuais começam com usuários abrindo um anexo, por exemplo”, relata.

Engrossa o coro Fabio Assolini, analista sênior de segurança da Kaspersky Lab. Segundo ele, ao treinar funcionários de departamentos não técnicos, orientando-os a identificar e encaminhar e-mails suspeitos para a TI poupa a empresa de problemas e elimina horas e horas de trabalho para apagar incêndios. “O fato humano ainda é bastante importante e não deve ser descartado”, relata.

Ele lista ainda outros quatro itens que as organizações devem cuidar de perto para reduzir drasticamente as chances de ataques virtuais. A primeira é manter um profissional dedicado que entenda do tema. “Esse talento precisa ser capacitado em segurança, pois ele vai lidar com um ativo de valor inestimável para as empresas: a informação”, comenta.

O segundo item de atenção, diz, está relacionado ao crescimento do BYOD. “A empresa precisa ter políticas de segurança, estabelecer como o acesso móvel será feito e de que forma as informações serão protegidas”, orienta. Para facilitar a gestão segura dos dispositivos, ele recomenda uma solução de mobile device management (MDM).

Assolini diz que hackers estão aproveitando vulnerabilidades de softwares antigos para invadir empresas. Por isso, é necessário sempre atualizar as soluções. “Um dos agravantes desse quadro no Brasil é a pirataria. Geralmente, quem tem software pirata desativa a atualização, tornando-se alvo para cibercriminosos.”

Por fim, ele recomenda uma solução de Application Control, que controla todos os softwares instalados no PC. “Por trás dessa tecnologia, há o Default Denied, que impede a execução de programas de arquivos desconhecidos na rede. Essa plataforma, presente em uma suíte de antivírus, evitaria, por exemplo, o ataque na rede da Sony Pictures”, pontua.

Falta regulamentação

Na opinião de Neto, Carraretto e Assolini, a falta de uma regulamentação em solo nacional que faça com que a empresa notifique publicamente invasões em seus sistemas, faz com que informações sobre riscos fiquem perdidas e não democratiza o acesso aos casos de ciberataques.

“Seria importante existir algo nesse sentido para aumentar a preocupação e a tratativa do tema. Como a companhia que teve dados violados vai lidar com o problema, qual o plano para endereçar?”, avalia Carraretto.

Para Neto, o fato de empresas no Brasil não relatarem problemas de segurança publicamente é uma questão cultural, barreira que precisa ser quebrada. “Se companhias dos Estados Unidos comunicam uma fraude, elas ganham credibilidade. No Brasil, ganha descrédito. Temos esse gap que precisa ser superado”, conta.

Ele lembra que o Marco Civil da Internet é um primeiro passo para mudar esse quadro e que a partir dele devem surgir leis para garantir mais transparência e processos para organizações reagirem de forma adequada aos ataques e até mesmo contribuírem para minimizar casos do tipo.

Fonte: IT Forum, em 10.02.2015.